



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,057	12/30/2003	Daryl Carvis Cromer	RPS920030222US1	7390
61755	7590	06/26/2007		
Kunzler & McKenzie 8 EAST BROADWAY, SUITE 600 SALT LAKE CITY, UT 84111			EXAMINER HENEGHAN, MATTHEW E	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 06/26/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/749,057	<b>Applicant(s)</b> CROMER ET AL.	
	<b>Examiner</b> Matthew Heneghan	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 30 December 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>12/30/03</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-30 have been examined.

***Information Disclosure Statement***

2. The following Information Disclosure Statement in the instant application has been fully considered:

IDS filed 30 December 2003.

***Specification***

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The term "computer readable storage medium" in claims 9-18 is not used in the specification.

4. The disclosure is objected to because of the following informalities: The list of inventors on the cover sheet of the specification is different from the list of inventors in the oath.

Appropriate correction is required.

***Claim Objections***

5. Claims 10-18 and 20-28 are objected to because of the following informalities: Each claim appears to be dependent upon the wrong claim. It is being presumed that claims 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 26, 27, and 28 are dependent upon claims 9, 10, 10, 9, 13, 9, 9, 9, 9, 19, 20, 20, 19, 19, 19, 19, 19, and 19, respectively. Appropriate correction is required.

Claim 16 is also objected to because it ends with a comma followed by a period.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 29 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. All of the means recited in claim 29 may be implemented in software; the claim therefore encompasses functional descriptive material that is not tangibly embodied.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2134

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 3 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims recite the Trusted Computing Group computer system specification. Since it is unclear what version of the specification is being referenced, or how a system would be considered to be in accordance with that specification, the scope of claims is indefinite.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 9-14, 17-24, and 27-29 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,058,807 to Grawrock et al.

As per claims 1 and 29, Grawrock discloses an embedded security system (a token) having PCRs record integrity metrics (measurement values) of processors (which

may be internal) and chipsets that are extended to the PCRs and seal cryptographic keys related to platforms (see column 5, lines 46-61). The chipsets may be devices physically connected to the computer system such as a disk drive (a data repository) (see column 4, lines 44-48).

As per claims 2, 4, 19, 20, 22, and 27, encryption operations relating to a data center (i.e. encryption and decryption) are performed using the cryptographic keys (see column 7, lines 1-19).

As per claims 9, 10, 12, and 17, the process is embodied in computer readable media (see column 6, lines 12-34).

As per claims 3 and 5, implementation is performed according to the TCG specification (see column 6, lines 10-16).

As per claims 11 and 21, the measurement is performed using a hash of the code (if it has firmware, then it is firmware code) (see column 5, lines 57-60).

As per claims 13, 14, 23, and 24, the unsealing of a key is done by the TPM by comparing the metric in the PCR to the current value (see column 10, lines 41-67).

Regarding claims 18 and 28, the TPM must be accessible without the sealed key, since it must be used to retrieve that sealed key.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 6-8, 15, 16, 25, 26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,058,807 to Grawrock et al. as applied to claims 4, 9, and 19 above, and further in view of U.S. Patent Application Publication No. 2005/0021968 to Zimmer et al.

Regarding claims 6, 7, 15, and 25, Grawrock discloses the use of disk drives, but not removable media per se.

Zimmer discloses that removable media and firmware (non-volatile) may be used for the platform device (see paragraph 13). One skilled in the art would recognize that using removable media affords greater security by allowing for storage of the security information apart from the computer.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a removable disk for the platform device, as disclosed by Zimmer, to afford greater security by allowing for storage of the security information apart from the computer.

Regarding claim 8, Grawrock does not disclose the test being performed before the operating system loads.

Zimmer discloses testing pre-boot so that the TPM functionality may be authenticated before system operation (see paragraph 17).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Grawrock by testing pre-boot, as disclosed by Zimmer, so that the TPM functionality may be authenticated before system operation.

Regarding claims 16 and 26, Grawrock does not disclose the use of serial numbers in the platform configuration.

Zimmer discloses the usage of serial numbers in platforms to identify the correct platforms for using firmware updates (see paragraph 47).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Grawrock by storing serial numbers on platforms, as disclosed by Zimmer, so that they can be used to identify the correct platforms for using firmware updates.

### ***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks

P.O. Box 1450

Alexandria, VA 22313-1450

**Or faxed to:**

(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Heneghan/

June 23, 2007

Patent Examiner (FSA), USPTO Art Unit 2134